The Institution of Railway Signal Engineers Inc

Australasian Section Incorporated

How Safe is Safe Enough? A Socio-technical View of Low-cost Level Crossing Safety

Christian Wullems
BIT(Hons) PhD MIEEE MACS
Cooperative Research
Centre for Rail Innovation

George Nikandros
BE CPEng FIRSE MIEAust MACS (Snr)
Australian Safety Critical Systems
Association

Peter Nelson-Furnell
B.Bus(Transport)
Public Transport Victoria

SUMMARY

Low-cost level crossings are often criticized as being unsafe. Does a SIL (safety integrity level) rating make the railway crossing any safer? This paper discusses how a supporting argument might be made for low-cost level crossing warning devices with lower levels of safety integrity and issues such as risk tolerability and derivation of tolerable hazard rates for system-level hazards. As part of the design of such systems according to fail-safe principles, the paper considers the assumptions around the pre-defined safe states of existing warning devices and how human factors issues around such states can give rise to additional hazards.

1 INTRODUCTION

Level crossings are a significant safety concern for Australian railways. Approximately 30% of rail related fatalities occurred at level crossings as a result of collisions between motor vehicles and trains for the five year period from 2001 to 2010 [1].

According to the railway level crossing stocktake conducted by RISSB in 2009 [2], there are 23,532 level crossings in Australia comprised of 8,838 public, 12,508 private, 566 maintenance and 1,659 pedestrian crossings (minus 39 that were counted twice).

Of these, approximately 33% of public, 0.5% of private, 1% of maintenance and 49% of pedestrian level crossings have a form of active protection. The remaining 79% of level crossings have passive protection and are typically found in low-population regional areas of Australia. Private and maintenance passive crossings however, are not restricted to low-population areas. While individually the risk at these crossings is insignificant, collectively they contribute to a significant proportion of the risk for railway operators.

In the ten-year period from 2000 to 2009, there were 695 collisions between trains and road vehicles at level crossings in Australia resulting in 97 fatal injuries [1]. Of these, 312 of the collisions occurred at level crossings with passive controls resulting in 39 fatal injuries.

The cost associated with upgrading these crossings, however, raises questions as to whether active treatments are warranted (practicable) given the relatively small risk.

This paper describes how an upgrade approach using low-cost warning devices can potentially provide a larger and earlier safety benefit for the population of level crossings with passive controls than using the current “standard” technology. In making a supporting argument for this approach, the question of how safe such warning devices need to be is posed, continuing the debate – how safe is safe enough in terms of risk acceptance.

While an understanding of what is tolerable in terms of hazard rates is useful in the specification of safety requirements for such systems, the paper also discusses fail-safe design principles and how these need to be considered in the context of varying operating conditions and human factors and how they can influence safety. The discussion focuses in particular on the effect reliability performance has on the level crossing user.

2 NOTATION

ALARP	As Low As Reasonably Practicable
ALCAM	Australian Level Crossing Assessment Model
ARO	Accredited Railway Operator
HSE	Health and Safety Executive, United Kingdom
LCLCWD	Low-cost Level Crossing Warning Device (assumes compliance with AS1742.7 [3] in relation to road signals e.g. RX5 light assemblies)

MTBF	Mean Time Between Failure
MTTR	Mean Time To Restoration
RAMS	Reliability, Availability, Maintainability and Safety
RISSB	Railway Industry Safety and Standards Board, Australia
RSSB	Railway Safety and Standards Board, United Kingdom
SFAIRP	So Far As Is Reasonably Practicable
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate

3 LOW COST RAILWAY LEVEL CROSSINGS

The Australian railway industry has been investigating low-cost railway level crossing warning devices (LCLCWDs) for several years as a possible control for the improvement of safety at low-exposure regional crossings across the network.

To eliminate the risk associated with the use of a different interface to the road crossing user, LCLCWDs will use the standard AS1742.7 [3] RX5 flashing light assembly road user interface so that from a road crossing user perspective, it will look like a standard configuration – i.e. nothing to differentiate LCLCWDs from conventional warning control devices. The key difference between LCLCWDs and conventional warning devices are the technologies used for power supply, train detection, connectivity and control. LCLCWDs are characterized by the use of technologies that reduce equipment, installation, maintenance and operating costs, and are often associated with lower levels of safety integrity [4].

Assuming LCLCWDs have a total cost of ownership that is approximately say 25% of the current “standard” technology, then an argument supporting the upgrading of a cross-section of passive (low-exposure) crossings with LCLCWDs is possible as more crossings can be treated for the same outlay; there is the potential for a significantly larger and earlier safety benefit for the population of crossings compared with an incremental upgrade approach using conventional warning devices, even allowing for a lower level of safety integrity for the LCLCWD [5].

One of the principles behind LCLCWDs is the utilization of devices with a level of safety integrity for safety-related functions (i.e. warn road user of approaching train) that is commensurate to the level of risk reduction required to meet the tolerable hazard rate (THR) for the hazard (collision between road vehicle and rail vehicle). As low-exposure crossings have a low risk, the magnitude of the risk reduction to sufficiently reduce the risk is less when compared to the magnitude of the risk reduction required for higher risk crossings.

Railway signalling technology existed long before the concept of safety integrity levels. Railway signalling has long been based on the fail-safe principle; and as such there is a tacit perception that all railway signalling technology is SIL4 (the highest safety level) because it is “fail-safe”. It is not the intention of this paper to debate the veracity of this perception.

The practice of requiring all railway-signalling equipment including railway level crossing warning devices to have a SIL4 rating (dangerous failure rate < 1E-8 / hour) for safety-related functions effectively creates a distortion in safety spending for sites where this level of risk reduction is an over-kill (no pun intended). A significant component of the cost of level crossing warning devices is influenced by safety integrity requirements; higher levels of safety integrity require more demanding development processes than lower levels and this is very much reflected in the relative development costs.

The following section poses the question, “how safe is safe enough?” and discusses the process of determining safety requirements for LCLCWDs based on European practice.

4 HOW SAFE IS SAFE ENOUGH?

The decision-making process for making safety-related decisions (i.e. deployment of LCLCWDs) would typically consider whether a risk control measure is legally required, and if not, whether the decision makes business or commercial sense. Consideration of the risk to individuals is typically part of the decision making process, prioritizing the risks that are evaluated for further risk reduction.

4.1 Legal Duty

Under Australian national rail safety legislation, railways are required to manage risk "so far as is reasonably practicable" (SFAIRP). The legislation states [6]:

> *“46—Management of risks*
>
> *A duty imposed on a person under this Law to ensure, so far as is reasonably practicable, safety requires the person—*
>
> *(a) to eliminate risks to safety so far as is reasonably practicable; and*

> *(b) if it is not reasonably practicable to eliminate risks to safety, to minimise those risks so far as is reasonably practicable."*

In determining what is reasonably practicable, the national rail safety legislation states [6]:

> *"47—Meaning of reasonably practicable*
>
> *In this Part—*
>
> *reasonably practicable, in relation to a duty to ensure safety, means that which is (or was at a particular time) reasonably able to be done in relation to ensuring safety, taking into account and weighing up all relevant matters, including—*
>
> *(a) the likelihood of the hazard or the risk concerned occurring; and*
>
> *(b) the degree of harm that might result from the hazard or the risk; and*
>
> *(c) what the person concerned knows, or ought reasonably to know, about—*
>
> *(i) the hazard or the risk; and*
>
> *(ii) ways of eliminating or minimising the risk; and*
>
> *(d) the availability and suitability of ways to eliminate or minimise the risk; and*
>
> *(e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk—the cost associated with available ways of eliminating or minimising the risk (including whether the cost is grossly disproportionate to the risk)."*

SFAIRP is defined in law and is assessed by a Court after-the-fact. The problem for railways is that they have judge before the fact that they can demonstrate to a future Court that the risk is SFAIRP i.e. after the harm has occurred.

4.2 Risk Tolerability

From the railway perspective, level crossings contribute significantly to the level of risk; however, from the road perspective, level crossings are considered to be of low if not insignificant risk due to the relatively low number of fatalities and injuries that occur at level crossings compared with those that occur on the road. From a societal perspective, it can be argued that compared to all causes of accidental death or injury, those that occur at railway level crossings are not significant [7]. While not related to the legal duty to ensure safety of the railway SFAIRP, the public perception of risk at level crossings and tolerability of high consequence occurrences with multiple fatalities needs to be taken into consideration (often termed societal risk tolerability). This poses the question: does society expect that it is practicable to eliminate level crossing collisions?

Events such as the collision between a truck and passenger train near Kerang in 2007 [8], resulting in 11 fatalities and 14 injuries, have the potential to drive policy changes that commit resources for prevention of future occurrences significantly exceeding what is economically reasonable (practicable) given the risk [9].

Individual risk tolerability also needs to be taken into consideration even though it is not directly related to the legal duty. In order to determine tolerability of a risk, the railway needs to have an understanding of what is acceptable and what is unacceptable [10].

In Australia there is no guidance as to the acceptable level of residual risk for level crossings, neither is there guidance on establishing limits of tolerability. It is left up to individual railway operators to define risk acceptance criteria.

The HSE in the United Kingdom provides general guidance on individual risk tolerability with a conceptual tolerability of risk framework setting boundaries between broadly acceptable and unacceptable risk [11].

In more recent guidance by the RSSB to the rail industry in the United Kingdom [12], it is noted that for risks approaching the unacceptable range, high priority should be given to the evaluation and development of options to reduce the risk, however only those that are reasonably practicable need to be implemented. The legal duty to reduce risk SFAIRP needs to be met irrespective of the level of risk incurred by exposed population groups. This appears to be consistent with the how the legal duty is interpreted in Australia.

As there is no legal requirement in Australia to consider risk tolerability, it is likely that many railways will not have quantitative risk acceptance criteria for level crossings.

Making an argument for the upgrade of a passive level crossing with a warning device will typically involve compliance with existing codes of practice and standards such as AS7658 [13] and AS1742.7 [3]. However, upgrading with a LCLCWD would mean installing a warning device with a lower level of safety integrity than existing "standard" warning devices – a level commensurate to the required level of risk reduction.

Therefore, an understanding of the limits of tolerability and where the current risk lies in relation to these limits is fundamental for determining what is an acceptable residual risk after treatment.

An example is provided below for a population of level crossings with passive controls in Queensland, suitable for upgrade with LCLCWDs.

Assessing each passively controlled crossing individually will more often than not result in no further action as the SFAIRP obligation is likely to have been met in that the cost of additional risk control measures is sufficiently disproportionate to the safety benefit. For this reason, the crossing population risk needs to be considered.

Nikandros in [14] suggests that the tolerability limit for a member of the general public of 1E-4 per year, as defined in guidance by the HSE in the United Kingdom, would seem reasonable for Australia based on Australian road fatality rates.

A hypothetical upper limit of tolerability for users of all level crossings in Queensland (excluding pedestrians) of 1E-4 is therefore apportioned to public passive level crossings, such that the individual risk for road users at all public passive level crossings in Queensland is:

1E-4 x 0.703 = 7.03E-5

where 70.3% of public level crossings in Queensland are passive [15]. One could argue that the 29.7% of active crossings are high-risk crossings and as such the apportionment should be biased such that the population of the public passive crossings should have a smaller risk budget. However for simplicity, no bias has been applied.

Using the lower bound of 1E-6 as a marker for acceptable risk, this apportioned value for road users at all passive level crossings in Queensland is:

1E-6 x 0.703 = 7.03E-7

The table below illustrates a crude analysis of current safety losses at passive level crossings in Queensland. Two sets of calculations were performed, one based on the number of registered vehicles in postal areas with passive level crossings, the other based on ALCAM survey data from a subset of passive level crossings whose traffic volumes had been surveyed.

The figures in the table below indicate that the current risk is approximately an order of magnitude lower than the hypothetical upper limit of tolerability 7.03E-5, however above the acceptable risk marker of 7.03E-7.

Number of public level crossings with passive controls	1269 in Queensland [15]	173 with ALCAM survey data
Vehicles	1,075,871 registered vehicles in postal areas with passive level crossings	29,488 surveyed traffic volumes
Assumed vehicle occupancy	1.1	
Assumed % of vehicles exposed to risk	20%	100%
Assumed % of vehicles exposed to risk that are regular users	70%	
Individuals regularly exposed to risk	165,684	22,705
Estimated annual collisions at all public passive LXs	6.3834 *(proportion of collisions that occurred from 2000-2009 at passive LXs 35.7% [1] x 161 collisions in QLD from 2001-2009 [16]) / 9 years*	
Estimated fatalities per collision at all public passive level crossings in Australia [1]	0.1411	
Estimated annual fatalities (no figures were available for injuries)	0.9007 (for population of passive crossings) *(6.3834 x 0.1411)*	0.1228 (for proportion of fatalities at surveyed passive crossings) *(173 x 0.9007) / 1269*
Individual risk for population of level crossings with passive controls in Queensland (annual fatalities / individuals regularly exposed)	**5.4363E-6**	**5.4085E-6**

4.3 Determining Tolerable Hazard Rates

Whilst there are standards for safety-related technology such as CENELEC EN50126 [17], EN50128 [18] [19], EN50129 [20] and IEC 61508 [21], their application is predicated on the amount of risk reduction that is desired. That desire depends on risk appetite and the ability to successfully argue that the risk has been reduced SFAIRP in a future Court. The standards do allow for risk treatments of varying effectiveness.

However, deciding which treatment/s to use depends on what one accepts as the residual risk.

A high-level description of the European approach to risk apportionment based on EN50126-2 [19] is described below (and illustrated in Figure 1).

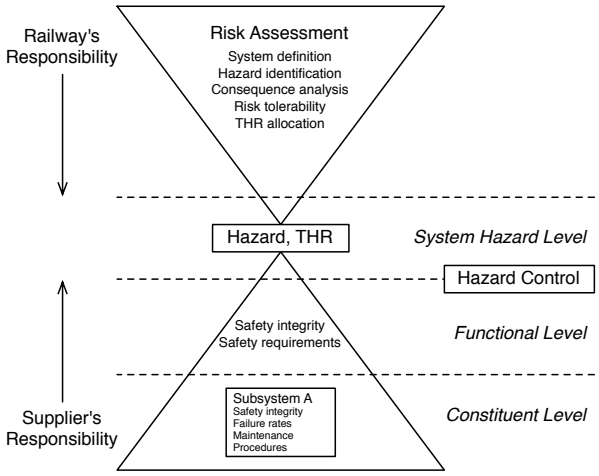


Figure 1. Typical safety requirement allocation process [19]

The railway is generally responsible for defining system level hazards and corresponding tolerable hazard rates (THRs). One approach described by EN50126-2 [19] involves the derivation of THRs by comparing the performance of existing systems, taking into account risk tolerability criteria. It is further noted that this can be facilitated either by analytical or statistical methods or from using qualitative approaches.

For example, the residual risk of level crossings with active warning systems in Queensland could be considered in the derivation of a THR for the hazard (collision between road vehicle and rail vehicle). This would mean that the magnitude of risk reduction required to meet the THR at a low-exposure passive level crossing would be less than at higher risk crossings, supporting the argument for LCLCWDs with a level of safety integrity commensurate to the required level of risk reduction to meet the THR.

Safety integrity relates to how often a safety-related system implementing a safety function can enter into an unsafe state that can lead to system level hazards, such that the hazard rate does not exceed the THR defined for the system level hazard. Safety integrity can be expressed as one of four discrete levels, SILs, where the apportioned THR falls within a range associated with a given level [19]. SILs are allocated to safety-related functions and consequently the subsystems implementing these functions. While random failures can be quantified using probabilistic calculations, this is not possible for systematic failures, and therefore each safety integrity level is associated with a group of methods and tools used to provide the stated level of confidence [20].

The SIL concept is commonly misused, especially for signalling equipment including level crossing warning devices. EN50126-2 [19] mentions several misuses including the use of SILs for marketing purposes, describing SILs as system attributes e.g. “a SIL4 level crossing warning system”, and derivation of THRs from SILs. Safety integrity requirements should be determined through the use of THRs as described above.

5 FAIL-SAFE DESIGN PRINCIPLES

Level crossing warning devices are designed with fail-safe principles [20], such that when a failure affecting the safety function is detected, the device enters or remains in a pre-defined safe state.

Failures of a system implementing the safety function (warn level crossing user of approaching train) can either be dangerous failures or safe failures, depending on the system state resulting from the failure. A dangerous failure is defined by IEC61508-4 [22] in continuous mode as a failure that:

> *“…causes a safety function to fail such that the EUC [Equipment Under control] is put into a hazardous or potentially hazardous state; or decreases the probability that the safety function operates correctly when required”*

An example of this type of failure is the undetected failure of the train detection function on the approach to a level crossing (e.g. approach track circuit fails wrong-side).

A safe failure on the other hand is defined by IEC61508-4 [21] as a failure that:

> *“results in the spurious operation of the safety function to put the EUC [Equipment Under Control] (or part thereof) into a safe state or maintain a safe state; or increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state”*

Safety integrity relates to the ability of a system to carry out the safety function(s) such that the higher the level of safety integrity, the lower the probability of a safety-related system failure affecting the safety function(s) or its ability to enter a safe failure mode [21]. The proportion of detectable dangerous failures to total dangerous failures by automatic on-line diagnostic tests is referred to as the diagnostic coverage of the system [21]. A high level of safety integrity alone does not imply a high level of reliability or availability. These are separate considerations that

need to be taken into account in terms of a how a system's reliability or availability may impact safety.

Safe failures, while technically safe when considered within the system boundary, can potentially impact the effectiveness of the control to reduce risk. How these "safe" failure modes affect safety (effective level of risk reduction in terms of hazard rate) when considered at the larger socio-technical system level depends largely on the operational and procedural context of the control.

CENELEC standard EN50126-2 [19] provides high-level guidance on designing fail-safe systems and details possible states in response to a failure (guidance on fail-safe design of electronic safety-related systems is given in EN50129 [20]). Of particular interest to this discussion is the "*system locked in a safe (restrictive) state"*, for which the guidance states that effectiveness of the system "lock-up" needs to be verified and a justification made that the state will not be cancelled due to additional failures.

It is further noted that:

> *"For justifying fail-safety at a system level, in addition to defining the system's safe state, the overall railway system should also be analysed as the resultant degraded modes may give rise to other hazards"*

Whether lock-up mode is inherent to the system or procedural, assurance needs to be made that further failures do not lead to unsafe states that are unacceptable to the safety requirements of the system. Consideration to this should not only be for further technical failures, but also human errors that could lead to additional hazards.

The safe state of existing Australian level crossing warning devices is the activation of the flashing lights and closure of the boom barriers (for level crossings with boom barriers). Of particular concern is compliance of the level crossing user. The road code - Queensland Transport Operations (Road Use Management—Road Rules) Regulation 2009 [23] specifically states in this case:

"A driver must not enter a level crossing if—

(a) warning lights (for example, twin red lights or rotating red lights) are operating or warning bells are ringing; or

(b) a gate, boom or barrier at the crossing is closed or is opening or closing; or

(c) …

Maximum penalty – 20 penalty units."

It is unlikely and unreasonable to expect level crossing users to wait indefinitely. This safe state therefore needs further consideration. The following section discusses human factors considerations of warning device failure modes.

6 HUMAN FACTORS CONSIDERATIONS OF WARNING DEVICE FAILURE MODES

While the safety integrity of technology performing safety-related functions is fundamental to ensuring safety, it is only part of the picture of a complex socio-technical system such as a level crossing warning system that has interfaces with other technical systems, and "non technical" systems e.g. level crossing users, train drivers, track workers, etc.

The performance of a warning system, its failure modes and its ability to clearly communicate its state to users of a level crossing can potentially condition their behaviour, resulting in an increase of errors or increases in non-compliant behaviour. This inturn can lead to an increase in the hazard (collision between road vehicle and rail vehicle) rate and thus reduce the level of risk reduction provided by the control.

There is often little consideration for how system performance outside the system boundary and at the interfaces with "non-technical" systems (i.e. humans) can affect overall safety performance.

Consideration of human factors in RAMS of a railway application is however prescribed by the CENELEC standard EN50126-1 [17]:

> *"Humans shall be considered as possessing the ability to contribute to the RAMS of a railway system. To achieve this aim, the manner in which human factors can influence railway RAMS should be identified and managed throughout the entire lifecycle. The analysis should include the potential impact of human factors of railway RAMS within the design and development phases of the system."*

And is additionally prescribed by the Australian Rail Safety National Law Regulations [24]:

> *"17—Human factors*
>
> *Procedures to ensure that human factor matters are taken into account during the development, operation and maintenance of the safety management system and for the integration of human factors principles and knowledge into all relevant aspects of operational and business systems."*

The following subsections discuss the effect of human factors on safety in relation to level crossing warning device failure modes.

6.1 Operational and Procedural Context

In a typical Australian regional scenario, an autonomous level crossing warning device with no rail-side healthy-state indication or level crossing approach signal is assumed. The remote monitoring system would be the timeliest source of failure information, communicating the failure state directly to the train control room via GSM. The maintenance response time would be typically less than 24 hours, however, in some very remote locations and in the case of multiple system failures in succession (e.g. due to severe weather conditions) this could be longer.

According to a draft version of the national code of practice for Australian Network Rules and Procedures (ANRP) being developed by RISSB [25], if an active level crossing is faulty or potentially faulty, network control officers must warn rail traffic crews. This communication would presumably occur via radio.

The rail traffic crew is required to approach the faulty level crossing at a speed that allows them to stop the rail vehicle short of the crossing for a suspected fault or confirmed fault where the crossing is unprotected, or protected by emergency services or road traffic controllers. The rail vehicle can proceed only if it is safe to do so. In the situation that a competent rail worker is protecting the crossing, the rail vehicle can proceed after the worker provides authorization to the rail traffic crew.

In the time that failure occurs to the time that the level crossing is protected for corrective maintenance and restored to a nominal operating state, level crossing users are exposed to a prolonged failure mode. Once level crossing users determine that no train is approaching, it is likely they will traverse the crossing after waiting for a period of time, driving around half-boom barriers (where applicable).

6.2 Human Performance

This section discusses human performance in relation to the level crossing user, the network control officer, the rail traffic crew and workers at the crossing; however, the discussion is limited to issues relating to reliability of the warning device.

Consider a level crossing warning device that is in one of the pre-defined safe failure states (flashing lights and lowering of boom barriers). The failure mode of Australian level crossings is indistinguishable from the train approach warning and does not provide feedback to the user as to the state of the system. When a level crossing user is first exposed, they are likely to assume that a train is approaching and wait. After the level crossing user realizes that no train is approaching, they find themselves in an unfamiliar situation and are unclear on what actions they should take. Inevitably, the level crossing user will traverse the crossing while the warning is active, which strictly speaking is non-compliant behaviour (non-compliant with road rules). On roads in regional areas on Australia, it is not uncommon to have level crossings on the only access road (i.e. no alternate routes in the case of a failure).

Factors such as poor sighting distance and bad weather (fog, rain, poor visibility) can compound the situation, significantly increasing the risk if trains are not stopped as a result of the failure.

A regular user may encounter the same level crossing failure several times in succession if it is a prolonged failure or on occasion if it is an intermittent failure. Frequent exposure to failure can condition the level crossing user to loose confidence in the warning, potentially affecting their performance at other level crossings as well. This is one of the hypotheses of a level crossing accident that occurred at Rungoo in 2008 [26], where the truck driver involved in the accident was exposed to a level crossing in a state of failure (continuous ringing) prior to the accident. It was noted by investigators that the driver's limited confidence that the warning indicated that a train was approaching might have contributed to the accident.

Intermittent safe failures (false alarms) have been found to influence the rate of non-compliance at level crossings [27]. In an observational study where 50% of warnings at one of the level crossings observed were false alarms [28], a high rate of non-compliance was observed compared with crossings with no false alarms. A simulator study conducted for the US Federal Railroad Administration [29] also concluded that motorists were sensitive to the reliability of the warning devices and were more likely to comply to signals when they perceived the warning to be reliable.

Performance shaping factors such as a level crossing user's expectation of when trains run (i.e. known schedules – especially for low rail traffic lines) are also expected to affect compliance. Coupled with exposure to failures, the level crossing user may create mental models of when the level crossing warning is credible, resulting in a mismatch between real risk and perceived risk, particularly when unscheduled trains are running.

Failure states where the warning device appears to operate correctly (i.e. warning was activated for an approaching train) have an even greater potential to mislead level crossing users. Failures such as tail ringing (failure to extinguish warning once a train has passed the crossing clearance point) can help create the false perception that it is safe to traverse the level crossing once the train has cleared the crossing. This becomes particularly dangerous when the extended delay is due to a second train instead of the warning. As

these types of failures directly influence level crossing user behaviour, they are more likely to be addressed in the warning device safety case.

From the perspective of stopping trains, the network control officer would have to receive an indication that a level crossing has failed or is not performing correctly. Depending on the coverage of remote monitoring system, some performance issues and types of intermittent failures may rely on analysis of logs or on-site inspections.

In evaluating the reliability of the procedure for stopping trains when a failure is detected, there are significant human performance issues and error producing conditions to be considered in how the network control officer becomes aware of the failure through a human machine interface (workstation in control room), the subsequent communications between the network control officer and the rail traffic crew, and the performance of the crew themselves.

An example of a few error producing conditions (identified in the Railway Action Reliability Assessment human reliability assessment method [30]) that can affect task performance are given below (non-exhaustive):

- *The need to transfer specific knowledge from task to task without loss:* A network control officer provides instructions to rail traffic crew in relation to level crossings that have a suspected failure. The train might be a significant distance from the suspected crossing(s), requiring the use of long-term memory;
- *An impoverished quality of information conveyed by person/person interaction*: Verbal communication (via radio) is used to inform rail traffic crew of level crossings that have a suspected fault. Information is complex and not well suited to verbal communication (i.e. codes, level crossing locations, etc.); and
- *Low signal to noise ratio:* Alarm flooding in the control room, especially in the case of lightning or whether events that can cause large numbers of simultaneous failures.

While warning device reliability and it effects on level crossing user performance has been discussed, in come contexts, the nominal operating performance of a warning device can also effect level crossing user performance.

For warning devices without a constant warning time function (i.e. provides constant warning time for approaching trains, irrespective of the train approach speed), the variation in warning time between different types of trains can be significant and influence level crossing user performance.

For example, if the majority of rail traffic consists of passenger trains, level crossing users might form mental models around the expected warning time. The warning time for the odd freight train operating at lower speeds could be significantly longer, resulting in a potential increase of non-complaint behaviour for longer warning times [27].

6.3 Determining Effective Level of Risk Reduction

While risk reduction can often be estimated using statistical models and operational data collected by railways, this is not always possible for the introduction of new technology or where performance (e.g. operating modes, reliability, availability, etc.) of a technology differs with respect to the reference technology on which such calculations are based.

In these cases, risk assessment using techniques such as event tree analysis and human reliability assessment, can provide an indication of where there are issues that need to be addressed. RSSB guidance on understanding human factors [31] reviews several techniques for evaluating human performance in the rail industry.

The amount of additional risk, in terms of system hazard (collision between road vehicle and rail vehicle) and additional hazards, can theoretically be calculated by summing the estimated additional risk for each failure mode from an analysis such as failure mode effect and criticality analysis (FMECA). Each failure mode with a quantified failure rate would be the initiating event for an event tree including probabilities for remote monitoring failure, human error probabilities for each task involved in ensuring level crossing is protected or trains are stopped and for human error probabilities related to users of the level crossing.

Where real-world data (task observation, incident data, simulation) is available, this should be used in preference to human reliability assessment.

There is limited evidence in the literature on the relationship between warning device reliability (MTBF), MTTR and how these affect level crossing user performance (error and non-compliance).

The CRC for Rail Innovation is investigating human performance of road users following exposure to prolonged and intermittent right-side failures at level crossings using driving simulation [32]. The aim of this research is to determine how these types of failure can condition road users and result in increased errors and non-compliance. The research also aims to discover whether road users' performance recovers once the warning system is restored to the nominal operating state. Data obtained from this research will be useful in informing the quantification of relationships between key parameters such as MTBF, MTTR

and the probability of road users making errors or engaging in non-compliant behaviour.

The driving simulator is a facility with a vehicle operating on a motion platform that provides six degrees of freedom immersed in a 180° virtual 3D environment. The use of a driving simulator offers a number of advantages including the provision of a safe and economical means of experimenting and facilitation of research that would otherwise not be possible due to ethical and safety issues.

In the absence of real-world data, human reliability assessment can be performed and involves performing a task analysis, identifying the errors that can arise in performing the task, development of a risk model for the task (typically a fault tree) and quantification of the model using human error probabilities. For railway procedures for example, human error probabilities can be quantified using a technique such as the RSSB Railway Action Reliability Assessment [30].

Sensitivity analysis methods such as Monte-Carlo simulation can be applied to provide a range of values taking into account variability of human performance in addition to technical failures.

6.4 Setting Appropriate Reliability Targets

This paper has discussed how reliability of level crossing warning devices can become a safety-related consideration, especially where human interfaces and procedures can give rise to hazards – both the system-level hazard (collision between road vehicle and rail vehicle) and additional hazards.

The human factors context is the least portable part of a safety argument and needs to be considered for the specific installation, procedural and operational context. In the case of LCLCWDs, such devices would be destined for installation at low population / low-exposure sites, typically rural areas of Australia where the response time and MTTR are likely to be longer.

By specifying reliability targets based on a specific deployment context, railways would be able to determine whether LCLCWDs that would otherwise meet safety requirements, would also meet the effective level of risk reduction required to meet the THRs associated with system-level hazards.

7 CONCLUSION

This paper introduced an argument for a level crossing upgrade approach using LCLCWDs. This approach can potentially provide a larger and earlier safety benefit than an incremental upgrade approach with existing “standard” warning devices for a population of passive level crossings, as more upgrades can be performed for the same budget.

Part of the cost reduction, however, is a result of the device being developed to a lower level of safety integrity. The paper continued the debate as to how safe is safe enough, discussing issues of risk tolerability and how THRs could be determined to support the SIL apportionment process.

Human factors considerations of warning devices and their interfaces between other technical systems and non-technical systems (e.g. level crossing users, train drivers, train controllers, etc.) were discussed in the context of fail-safe design principles and the pre-defined safe failure states of existing “standard” warning devices.

The paper challenged the validity of assumptions underpinning safe failure states and discussed a high-level methodology for determining the effective level of risk reduction of warning device, taking into account human factors issues that can give rise to the system-level hazard (collision between rail vehicle and road vehicle) and additional hazards.

8 REFERENCES

[1] Independent Transport Safety Regulator. (2011, 23/01/2012). Level crossing accidents in Australia. *Transport Safety Bulletin*. Available: http://www.transportregulator.nsw.gov.au/rail/publications/transport-safety-bulletins/level-crossing-accidents-in-australia/view

[2] Railway Industry Safety and Standards Board, "Level Crossing Stocktake," 25 May 2009 2009.

[3] Standards Australia, "AS1742.7-2007 Manual of uniform traffic control devices Part 7: Railway crossings," ed, 2007.

[4] C. Wullems, "Low Cost Railway Level Crossings," in *Confrence on Railway Engineering (CORE2012)* Brisbane, Australia 2012.

[5] C. Wullems and G. Nikandros, "Adoption of Low-Cost Rail Level Crossing Warning Devices: An Australian Case Study," in *Railway Safety, Reliability and Security: Technologies and Systems Engineering*, F. Flammini, Ed., ed Pennsylvania, USA: IGI Global 2012.

[6] *Rail Safety National Law (South Australia) Act 2012*, 2013.

[7] P. Hughes, "Booms go bust," *International Railway Journal,* vol. 52, pp. 37-39, 2012.

[8] Office of the Chief Investigator - Transport and Marine Safety Investigations, "Rail Safety Investigation Report N° 2007 / 09: Level Crossing Collision - V/Line

Passenger Train 8042 and a Truck Near Kerang, Victoria - 5 June 2007," Melbourne, Australia 2008.

[9] C. Wullems, N. Haworth, and A. Rakotonirainy, "Human Factors at the Interface Between Road and Rail," in *Advances in Human Aspects of Road and Rail Transportation*, ed: CRC Press, 2013.

[10] L. Neist. (2011) Weighing up the risk factors. *Track & Signal*. 36-37.

[11] Health and Safety Executive, "Reducing Risks, Protecting People - HSE's decision making process," Norwich, United Kingdom 2001.

[12] Railway Safety and Standards Board (RSSB), "Taking Safe Decisions - how Britain's railways take decisions that affect safety," London, UK 2009.

[13] Railway Industry Safety and Standards Board (RISSB). (2012). *AS7658 Infrastructure - Railway Level Crossing*. Available: http://www.rissb.com.au/site/products_control.php?document=7658

[14] G. Nikandros, "Signalling So Far As Is Reasonably Practicable," presented at the IRSE AGM Technical Convention, Brisbane, 2010.

[15] Department of Transport and Main Roads, "Dataset of level crossings in Queensland," ed. Brisbane, 2011.

[16] Australian Transport Safety Bureau, "Australian Rail Safety Occurrence Data 1 January 2001 to 31 December 2009," Canberra 2009.

[17] CENELEC - European Committee for Electrotechnical Standardization, "EN50126-1 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process," ed, 2006.

[18] CENELEC - European Committee for Electrotechnical Standardization, "EN50128 Railway applications - Communication, signalling and processing systems: Software for railway control and protection system," ed, 2001.

[19] CENELEC - European Committee for Electrotechnical Standardization, "EN50126-2 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)- Part 2: Guida to the application of EN 50126-1 for safety," ed, 2007.

[20] CENELEC - European Committee for Electrotechnical Standardization, "EN50129 Railway applications - Communication, signalling and processing systems: Safety related electronic systems for signalling," ed, 2003.

[21] IEC - International Electrotechnical Commission, "61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements," ed, 2010.

[22] IEC - International Electrotechnical Commission, "61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations," ed, 2010.

[23] *Queensland Transport Operations (Road User Management--Road Rules) Regulation*, 2009.

[24] *Rail Safety National Law National Regulations 2012*, 2013.

[25] Railway Industry Safety and Standards Board (RISSB), "ANRP 2015 Active Control Level Crossing Management," in *Australian Network Rules and Procedures (ANRP)*, ed, 2011.

[26] Department of Transport and Main Roads, "Final Report - Rail Safety Investigation - QT2459: Fatal Collision between the Cairns Tilt Train and B-Double Truck, Rungoo Level Crossing, Queensland, 27 November 2008," Brisbane, Australia 2009.

[27] M. Yeh and J. Multer, "Driver Behavior at Highway-Railroad Grade Crossings: A Literature Review from 1990-2006," U.S. Department of Transportation Federal Railroad Administration, Washington DC, USA DOT/FRA/ORD-08/03, 2008.

[28] J. N. Brites, M. C. Hay, and G. J. S. Wilde, "Video-recorded Driver Behaviour at Railway Crossings: Approach Speeds and Critical Incidents," Canadian Institute of Guided Ground Transport Report No. 87-7, 1987.

[29] M. Gil, J. Multer, and M. Yeh, "Effects of Active Warning Reliability on Motorist Compliance at Highway-Railroad Grade Crossings," U.S. Department of Transportation Federal Railroad Administration, Washington DC, USA DOT/FRA/ORD-09/06, 2007.

[30] H. Gibson, "Railway Action Reliability Assessment User Manual: A technique for

the quantification of human error in the rail industry," Rail Safety and Standards Board London, UK 2012.

[31] Railway Safety and Standards Board. (2008). *Understanding Human Factors - a guide for the railway industry (2nd ed.)*. Available: http://www.rssb.co.uk/EXPERTISE/HF/Pages/HUMANFACTORSGOODPRACTICEGUIDE.aspx

[32] M. Gildersleeve and C. Wullems, "A Human Factors Investigation into the Unavailability of Active Warnings at Railway Level Crossings," in *ASME/ASCE/IEEE 2012 Joint Rail Conference (JRC2012)*, Philadelphia, USA, 2012.

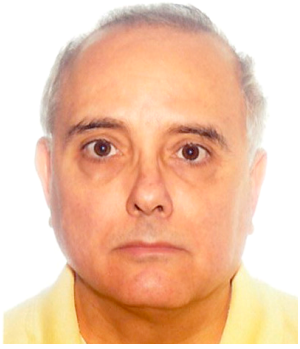
AUTHORS

Christian Wullems

Chris is a postdoctoral researcher with the CRC for Rail Innovation in Australia. He is currently leading several collaborative industry projects in the area of rail safety. The projects range from a national trial and evaluation of risk and legal arguments for low-cost level crossing warning devices to improving safety data through the capture of objective precursor data using analysis of train event logs and video analytics with forward facing video.

Prior to his present appointment, Chris was the technical director of Qascom S.r.l., Italy, managing research on anti-spoofing techniques for civilian global navigation satellite system receivers. He received his Ph.D. from the Queensland University of Technology, where he investigated security of wireless communications and location acquisition systems including GPS for critical applications.

Chris has published several papers in the areas of global navigation satellite systems, cryptography, network security, telecommunications and railway level crossing safety.



George Nikandros

George Nikandros is an electrical engineer with some 35 years experience in the railway signalling industry.

He was a foundation member of the Australian Computer Society's National Technical Committee on Safety-Critical Systems when it was established

in 1992; a committee, which evolved into the Australian Safety Critical Systems Association in 2002. He chaired that association from its inception in 2002 until June 2010.

He is a member of the Railway Technical Society Australasia and member of the Queensland chapter committee since its formation in 1998 and chaired that committee from 1999 to 2004.

He is a Chartered Member of Engineers Australia, a Fellow of the Institution of Railway Signal Engineers, a Senior Member of the Australian Computer Society and member of the Risk Engineering Society.

George has published papers and a co-author of the book “New Railway Environment – A multi-disciplinary business concept”.

Peter Nelson-Furnell

Peter Nelson-Furnell is the Manager Railway Crossing Safety for Public Transport Victoria and the Chair of the national Australian Level Crossing Assessment Model committee.

He has been involved in the construction and risk assessment of level crossings from Australian National in the 1980’s through to his current role in managing the Victorian level crossing safety programs. He is a key developer of level crossing risk tools and champions various innovative level crossing technology trials through the Rail and Auto CRCs.